April 25, 2012	The SMOS Initiative was an off-time activity of Finnish science and technology professionals interested in creating innovative solutions for disaster communications.

SMOS 6: Technical goals: system requirements

STARTING POINT

This document describes system requirements and logical structure of the SMOS system. A separate document (SMOS 7) is planned to discuss more about potential hardware of SMOS bases station module.

As described in the SMOS discussion paper (SMOS 2), it was found that during major disasters, communications networks tend to become nonfunctional for the first 72 hours or so, before they gradually start to recover. It was also found that local emergency responders are likely to be victims themselves, thus not being able to help their community. For the first hours, any lives that are saved are saved by the victims themselves. The external world has great difficulty in obtaining correct situational awareness to tailor the aid that will be later be sent to the emergency destination.

Due to the above findings, we claim that empowering the local people with communications possibilities during the emergency situation would help save a significant number of lives. This would happen via 1) by the local people during the first 72 hours and 2) by the correctly prioritized and planned aid starting to arrive during the next following days.

SYSTEM LEVEL USABILITY REQUIREMENTS

This section lists what service levels and features should be achieved on a 72h civil emergency communications system to make suitable for its purpose. These system level usability requirements are divided into breakable and unbreakable items. A design must meet all unbreakable requirements to be feasible for the targeted use case.

Unbreakable

- **RQ1:** system shall allow people to communicate with each other when conventional communications systems have failed
- **RQ2**: system shall be in operation 24 hours after the ground zero, at latest
- **RQ3:** system shall able to operate 72 hours without external power sources
- **RQ4:** system shall be easily deployable by trained volunteers
- **RQ5:** system does not require any special skills from the victims to communicate that they do not already have prior to the disaster
- **RQ6:** system shall provide connectivity to the external word, for help requests and to support building of situational awareness
- **RQ7:** system shall provide competitive Return Of Investment in terms of saved lives per dollar when compared to other ways of using aid money

Breakable

- system should be able operate locally without connection to external world, if not available
- system should provide useful information proxies for the situational awareness, such as maps on victim locations and their movements
- system should support SMS cell broadcast (SMS-CB) to population at certain area
- system should support information-on-demand type of services, SMS polls and surveys

- system should provide interface to external sensor devices, such as Geiger counter.

BUDGETARY CONCERNS

It is not exactly known how much a system is allowed to cost. It is however known that many help organizations operate on a relatively small budgets. Even larger ones cannot risk their aid money in the development of a system whose benefits are not already proved in practice. In the absence of a traditional business case, the team is also short of funding. In many ways it seems evident, that for a system to be successful, it must be very, very, affordable when compared to traditional telecom offerings. From this perspective, it does not make sense to explore technological choices that for instance involve heavy licensing fees or hardware costs.

At the same time it should be noted that this budgetary guidance might not be a problem for the big telecom infrastructure players. They would be able use their existing IPR “for free”. In the most optimal case, the required system components would have already been developed for some other applications (such as sensor swarm networks) and economies of scales would be pushing manufacturing costs down. Showing a corporation's social responsibility might be another reason to invest on this technology in spite of weakish business case.

In this document, however, we will focus on technology options that are available for the greater audience. “Availability” means that a group of technology enthusiasts and volunteers would be able to purchase all required components to develop a Proof Of Concept. Aim of this approach would be to show that the SMOS concept is possible and that it would deliver claimed benefits.

SYSTEM PROPOSAL

A key to make an emergency communications system cost-efficient is to cut the energy consumption in every possible way. Small power consumption leads to smaller required accumulator capacity, making units consequently smaller and lighter in weight, thus making transportation of equipment more affordable (and even possible in locations where all roads are lost and airfields ruined).

To meet the listed requirements, we suggest implementing a small base station module that only supports SMS traffic. This would perfectly match RQ5, as users would use the equipment that is already near to them when a disaster occurs and they are familiar with -- their own cell phones. The proposed solution is slightly lacking in fulfilling RQ1, as writing text messages may not be most convenient way of communication. It is however expected that even in the poorest countries SMS is well known application as sending SMS is typically more affordable than traditional voice calling. There is also a push in various developing countries, for example Sri Lanka, to require communication in disasters to occur only via SMS to avoid congestion. Thus, we can assume that SMS is familiar enough.

We expect to meet RQ4, if the system is designed to work autonomously from the ground-up. It must not require any cumbersome on-field configuration work. In other words, the system must be “drop-and-go” ready. A SMS-only basestation unit would not need to support GSM Traffic Channels (TCH), which is expected to decrease a BS complexity and power budget significantly. A BS however still needs to continuously transmit a carrier signal for cell phones to detect it, making the BS consume power constantly, when in-service.

Alternative system proposal I – VHF radio dropping

The team considered whether direct air-dropping of conventional VHF radios would do the job. A major problem with this approach is that helper organizations themselves rely on VHF radios in their field operations, the voice traffic being largely unencrypted. More traffic on VHF bands would have a significant negative impact on their own operations. In addition, although the simplest VHF radio models might be taught in a minute for a person to learn basic use, it still initially requires someone to show how the radio works. Figuring out new technology just by one's intuition is not really a sustainable assumption, considering that the disaster victims are at the same time under a heavy stress.

Alternative system proposal II – smoke detector analogy

Team considered whether households should be equipped with SMOS modules in the same way as they are nowadays equipped with smoke detectors. In some countries households already have base stations inside, called femtocells. Basically adding a battery backup to such femtocell would do the job. Unfortunately the link to external world is typically handled with ADSL modem utilizing conventional telephone cabling. In disasters of the type we are contemplating, the ADSL line would almost by definition be prone to get cut. In addition, base stations would be buried inside collapsing buildings, limiting their radio range. Affordable femtocells are based on 3G technology, making them unusable in less developed countries. This option might still be feasible in most developed and populated countries having a high risk of a disaster, such as Japan. This approach however is not viable as a common solution to the problem.

INTERFACES

From down to up, the proposed system has the following interfaces and relating functionalities.

GSM Air (Um) Interface

Partial implementation of the Air-interface to support SMS-messaging is required. Paging Channel (PCH) is used to inform mobile host about incoming SMS message. Mobile host uses Random Access Channel (RACH) to inform its availability to receive SMS message. Standalone Dedicated Control Channel (SDCCH) is established to convey the SMS message to a mobile host. No Traffic Channels (TCH) support is needed as voice or data calls are not supported.

A SMOS base station needs to support following GSM transactions: Radio channel establishment, Location updating, Mobile-Originated SMS, and Mobile-Terminated SMS.

Adjacent GSM radio channels do overlap, thus some clever-minded engineering work is needed to develop automated self-configuration mechanism of neighboring cells. BS-nodes will need to discover their neighboring cells via ad-hoc radio connection mesh, and then agree mutually that various base station and cell identifiers are unique and that frequencies of the neighboring cells do not overlap.

To further avoid on-field configuration work, SMOS bases stations would default to pretend foreign network operator to the local GSM subscribers. Mobile handsets would then roam to international network having different Mobile Country Code. SMOS base stations would need to monitor the radio spectrum and automatically switch off the radio transmission module when the local cellular network recovers back to operation.

Connection Mesh Interface between the SMOS basestations

A routing protocol with fully decentralized knowledge about the best route through the network (such as B.A.T.M.A.N) running on top of wireless ad-hoc links, (such as IEEE 802.11g).

It would not be viable to run a standard A-bis interface on top of the connection mesh, as it would rapidly drain the base station's batteries. Most of the Air interface queries should be cached, or even faked, to decrease needed uplink communication. Instead, a special kind of emergency protocol would need to be implemented that will cut the communication needs to an absolute minimum. As a basic principle, the radio mesh should wake-up periodically and all queries should be buffered during silent period. When radio is again switched on, the buffered queries should then be sent in larger chunks, not one-by-one. Once the buffers are flushed, radio is again switched off immediately. For a new base station to connect to the existing mesh, it needs to first monitor the “pulse” of the radio mesh and then start communicating on same sync.

SMOS uplink interface

SMOS uplink gateway would provide a conventional TCP/IP up-link connection to the external world. Payload transmitted within the TCP/IP pipe can be encrypted. Each SMOS base station could be basically equipped with well supported RJ-45 Ethernet port to connect to any such available equipment providing DHCP service and access to the Internet. In that sense, SMOS uplink-gateway can be a COTS component, not requiring any own development work. During a major disaster, the only viable way to arrange access to the Internet might be by satellite phone technology. In less severe circumstances, a wide range of another Internet access technology could be utilized, depending on their local availability. At minimum, one SMOS base station in the local mesh would need to have uplink access. In case uplink access is lost, SMOS base stations would still allow SMS-communication locally. Inside the TCP/IP uplink connection, the same bandwidth savvy “SMOS emergency protocol”, as used between the base stations, would be tunneled to SMOS backend server. Exception being that the link to outer world is assumed to be bottleneck due to its potentially low bandwidth. Thus, the link would likely need to be active all the time to carry as much buffered traffic trough as possible. The SMOS base station taking care of uplink access would as well likely need to be equipped with external battery or other power source due to its higher traffic load. The edge base station could share the same external power source as uplink satellite communication system is using.

SMOS operator interface

The task of the backend server is to convert minimalistic SMOS signaling to more verbose standard based telecom messaging, to integrate with the real world GSM network. Utilization of SMOS (satellite) uplink is also minimized on this side of the uplink interface, as SMOS backend server will on its behalf cache messaging between the outside world and SMOS base stations.

The SMOS backend server must be located in a safe location (perhaps even a foreign country), where the risk of any kind of disaster is small. SMOS backend server must be configured and functional already before the disaster occurs. Configuration work of traditional telecom network is a time consuming task and starting this work from scratch would hurt our 24h response time requirement 'RQ2'. Geographical location of backend server should not limit as itself deployment of SMOS emergency network anywhere in the globe.

The backend server could in principle directly integrate to the SMOS companion operator's network architecture. In this arrangement it would look like local subscribers would have suddenly teleported themselves to the foreign country and then roamed to the operator's network on this foreign country. For this approach to work, core network elements of the disaster area operator would still need to be functional and accessible from the foreign country. SMS charging would work as usual, providing income to operators according to their existing mutual agreement.

GSM core network usually resides in a stronghold, but the lines to the external world introduce a risk that HLR or local Short Message Service Centre (SMSC) may not be reached, despite the usual redundant signaling routes. In such a case, IMSI querying of subscriber's MSISDN (phone number) would fail. Conventional GSM infrastructure has not been defined to cope with this situation, a subscriber cannot get network service, nor exchange SMS messages with the outside world.

An alternative method would be to integrate the SMOS backend server to a SMS-gateway of one of the SMS-bulk messaging companies. The best bulk messaging providers have nearperfect operator coverage, including hard-to-reach regions like Haiti. Integration is made temptingly easy by providing straight-forward HTTP/S based API, in contrast to tratidional SS7 based telecom signaling. This approach makes SMS messaging possible even if home country's GSM core network is out of reach, but does not solve problem of not being able to retrive subscriber's MSISDN number. In this unfortunate case MSISDN would need to be queried directly from the user “please reply, what is your phone number?”. A user can easily give false identity, a catch being that a SMOS base station records user's unique IMSI and it is thus possible to identify the true identity of the wrong doers and also block them as soon as connectivity to the HLR is restored. With technique called SMS-spoofing (known from Skype), Message can be made look real on the receiver's phone, but GSM network sides notes the difference and may or may-not allow sending replies back to the SMS gateway. It might be safer to reserve an own (short) number for SMOS and use it as a legitimate Sender ID. In addition, an separate SMS message can be send automatically to inform the receiver that only replying to original message works and the SMS did come from the disaster area, from this assumed phone number. Sending SMS to disaster area without possibility to reply-back requires some additional arrangement, like filling the receiver's number to the begin of the SMS message.

On this SMS Gateway based approach it might be practically impossible to charge from SMS messaging traffic that is sent from disaster area towards outer-world. SMS Gateway service provider is still charging the SMOS service provider from each forwarded message. As a potential workaround, replying back to SMOS emergency short number could be made to cost enough to cover all expected costs.